WireShark HTTP

1. The browsing running HTTP version is 1.1

2. English

3. 192.168.1.101 IP address of client

128.119.245.12 IP address of server

4. The status code returned from the server to the client is 200

5. The HTML file was last modified from the server at Wed, 26 Feb 2014 02:17:01

6. The number of types returned from the server is 428

7.

8. In the first HTTP get request from the server to the client, there is no “IF-MODIFIED-SINCE” line

9. The serer explicitly returns the content of the file by the response phrase “ok” and the status code is 200 which indicates it is from the server.

10. If-Modified-Since: wed, 26 Feb 2014 03:52:01 GMT\r\n

11. The status code is 304 and the response phase is “Not Modified”. From this, we could tell this the second request response was not from the server, it is from the cache instead.

12. Only one HTTP GET request message was sent to the server and the packet number is 76.

13. The last one which is 87 contains the status code and the response phrase.

14. 200 and ok.

15. There are 4 pieces of TCP segments needed to carry one single HTTP response and the text of the Bill of Right.

16. There are 4 HTTP GET requests were sent to destination, 128.119.245.12, 165.193.140.14, 128.119.240.90, 128.119.240.90.

17. By looking at the time of when the requests are made, we know that the image were download serially.

18. The first response phrase is “Authorization Required” and the status Code is 401.

The Second response phrase is “ok” and the status code is 200.